IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

JOSHUA HENDERSON, individually and on behalf of all others similarly situated, Plaintiff, **AHOLD DELHAIZE USA SERVICES, LLC, FOOD LION, LLC, and GIANT FOOD, LLC,** Defendants,	**No.** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Joshua Henderson ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendants, Ahold Delhaize USA Services, LLC, ("Ahold"), Food Lion, LLC ("Food Lion"), and Giant Food, LLC ("Giant Food") (collectively "Defendant"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to his own actions, and upon information and belief and his counsel's investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendants with sensitive Personally Identifiable Information ("PII"[1]) and Protected Health Information ("PHI" or "Private Information") that was impacted in a data breach that Defendant publicly disclosed in June 2025 (the "Data Breach" or the "Breach").

2. Defendant Ahold is the largest grocery retail group on the east coast and the fourth

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

largest in the United States.[2]

3. Defendant Food Lion is an American regional supermarket chain headquartered in Salisbury, North Carolina. Defendant Food Lion is a subsidiary of Defendant Ahold.

4. Defendant Giant Food is an American regional supermarket chain headquartered in Landover, Maryland. Defendant Giant Food is a subsidiary of Defendant Ahold.

5. Plaintiff and Class Members are current and former employees of Defendants.

6. Defendants had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

7. On November 6, 2024, Defendant Ahold detected a cybersecurity issue involving unauthorized access to some of its internal U.S. business systems.[3] In response, Defendant Ahold launched an investigation to determine the nature and scope of the Data Breach.[4]

8. Defendant Ahold's investigation determined that an unauthorized third party obtained certain files from one of its internal U.S. file repositories between November 5 and 6, 2024.[5] Based on a review of the impacted files, Defendant Ahold determined that some of the files may have included internal employment records containing personal information obtained in the course of providing services for certain current and former Ahold Delhaize USA companies, including Defendants Food Lion and Giant Food.[6]

9. Upon information and belief, the following types of Private Information may have

[2] Niamh Ancell, *Ahold Delhaize USA confirms 2M+ victims affected by 2024 cyberattack*, https://cybernews.com/security/ahold-delhaize-usa-cyberattack-affects-millions/ (last visited June 27, 2025).
[3] Sample Notice Letter, https://www.maine.gov/cgi-bin/agviewerad/ret?loc=2753 (last visited June 27, 2025).
[4] *Id.*
[5] *Id.*
[6] *Id.*

been impacted in the Data Breach: name, contact information (for example, postal and email address and telephone number), date of birth, government-issued identification numbers (for example, Social Security, passport and driver's license numbers), financial account information (for example, bank account number), health information (for example, workers' compensation information and medical information contained in employment records), and employment-related information.[7]

10. On June 26, 2025, Defendant Ahold issued a notice of public disclosure about the Data Breach and began sending notice letters to individuals impacted.[8]

11. Defendants failed to safeguard individuals' highly sensitive Private Information.

12. Plaintiff and Class Members now face a lifetime risk of identity theft due to the nature of the information lost, which they cannot change, and which cannot be made private again.

13. Defendants harmful conduct has injured Plaintiff and Class Members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; (iv) invasion of their privacy; (v) loss of the benefit of the bargain; and (vi) emotional distress associated with the loss of control over their highly sensitive Private Information.

14. Defendants' failure to protect individuals' Private Information has harmed and will continue to harm Plaintiff and Class Members, causing Plaintiff to seek relief on a class wide basis.

15. On behalf of himself and all others similarly situated Plaintiff brings causes of action against Defendants for negligence, negligence *per* se, breach of implied contract breach of

[7] *Id.*
[8] *Data Breach Notifications*, Office of the Maine Attorney General, Ahold Helhaize USA Services, LLC: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b17963fc-3806-430e-b28e-bac47eb73a8b.html (last visited June 27, 2025).

confident, and unjust enrichment, resulting from Defendants failure to adequately protect their highly sensitive Private Information.

PARTIES

16. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the State of Virginia.

17. Defendant Ahold is a Limited Liability Company organized under the laws of the State of Delaware with its headquarters and principal place of business at 2110 Executive Dr, Salisbury, North Carolina, 28147.

18. Defendant Food Lion is a Limited Liability Company organized under the laws of the State of North Carolina with its headquarters and principal place of business at 2110 Executive Drive, Salisbury, North Carolina, 28147.

19. Defendant Giant Food is a Limited Liability Company organized under the laws of the State of Maryland with its headquarters and principal place of business at 6300 Sheriff Road, Landover, Maryland, 20785.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Members of the proposed Classes are citizens of different states than Defendants, and there are over 100 putative Class Members.[9]

[9] *Data Breach Notifications*, Office of the Maine Attorney General, Ahold Helhaize USA Services, LLC: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b17963fc-3806-430e-b28e-bac47eb73a8b.html (last visited June 27, 2025).

21. This Court has personal jurisdiction over Defendants because Defendants Ahold and Food Lion are headquartered in this District, regularly conducts business in this District, and have sufficient minimum contacts in this District.

22. Venue is proper in this Court because Defendants Ahold and Food Lion have their principal offices is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

Defendants Business

23. Defendant Ahold is the largest grocery retail group on the east coast and the fourth largest in the United States.[10]

24. Defendant Food Lion is an American regional supermarket chain headquartered in Salisbury, North Carolina. Defendant Food Lion is a subsidiary of Defendant Ahold.

25. Defendant Giant Food is an American regional supermarket chain headquartered in Landover, Maryland. Defendant Giant Food is a subsidiary of Defendant Ahold.

26. Plaintiff and Class Members are current or former employees of Defendants.

27. Upon information and belief, as a condition of obtaining employment, Plaintiff and Class Members, were required to provide sensitive and confidential Private Information, including their names, addresses, Social Security Numbers, dates of birth, tax identification numbers, driver's license numbers or state-issued identification card numbers, passport numbers, other government-issued identification numbers, financial account information, payment card information, medical information, and health insurance information, and other sensitive information, that would be held by Defendants in their computer systems.

[10] Niamh Ancell, *Ahold Delhaize USA confirms 2M+ victims affected by 2024 cyberattack*, https://cybernews.com/security/ahold-delhaize-usa-cyberattack-affects-millions/ (last visited June 27, 2025).

28. The information held by Defendants at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

29. Upon information and belief, Defendants made promises and representations to individuals that the Private Information collected would be kept safe and confidential, and the privacy of that information would be maintained.

30. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

32. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendants had a legal duty to keep individuals Private Information safe and confidential.

33. Defendants had obligations under the FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

34. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendants would be unable to offer employment and in turn render their services.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

The Data Breach

36. On November 6, 2024, Defendant Ahold detected a cybersecurity issue involving unauthorized access to some of its internal U.S. business systems.[11] In response, Defendant Ahold launched an investigation to determine the nature and scope of the Data Breach.[12]

37. Defendant Ahold's investigation determined that an unauthorized third party obtained certain files from one of its internal U.S. file repositories between November 5 and 6, 2024.[13] Based on a review of the impacted files, Defendant Ahold determined that some of the files may have included internal employment records containing personal information obtained in the course of providing services for certain current and former Ahold Delhaize USA companies, including Defendants Food Lion and Giant Food.[14]

38. Upon information and belief, the following types of Private Information may have been impacted in the Data Breach: name, contact information (for example, postal and email address and telephone number), date of birth, government-issued identification numbers (for example, Social Security, passport and driver's license numbers), financial account information (for example, bank account number), health information (for example, workers' compensation information and medical information contained in employment records), and employment-related

[11] Sample Notice Letter, https://www.maine.gov/cgi-bin/agviewerad/ret?loc=2753 (last visited June 27, 2025).
[12] *Id.*
[13] *Id.*
[14] *Id.*

information.[15]

39. On June 26, 2025, Defendant Ahold issued a notice of public disclosure about the Data Breach and began sending notice letters to individuals impacted.[16]

40. Defendants failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

41. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiff and Class Members. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

42. Plaintiff further believes his Private Information, and that of Class Members, was subsequently published and sold on the dark web following the Data, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable.

43. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

44. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection. "[17]

[15] *Id.*
[16] *Data Breach Notifications*, Office of the Maine Attorney General, Ahold Helhaize USA Services, LLC: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b17963fc-3806-430e-b28e-bac47eb73a8b.html (last visited June 27, 2025).
[17] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 10, 2025).

45. To prevent and detect cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. [18]

46. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

[18] *Id.* at 3-4.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

47. Given that Defendants were storing the sensitive Private Information of their current and former employees, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

48. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, millions of individuals, including that of Plaintiff and Class Members.

Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information.

49. As a condition of employment, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendants.

50. Defendants retain and store this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendants would be unable to would be unable to offer employment and in turn render their services.

51. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they was responsible for protecting the Private Information from disclosure.

52. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private

[19] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited June 10, 2025).

Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

53. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

54. Upon information and belief, Defendants made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

55. Defendants' negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Knew or Should Have Known of the Risk of a Cyber Attack Because Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks

56. Data thieves regularly target entities like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

57. Defendants data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities like Defendants that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

58. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January

2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

59. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[20]

60. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[21] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[22] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[23]

61. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

---

[20] *Id*.

[21] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report/.

[22] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[23] *See id.*

62. Additionally, as companies became more dependent on computer systems to run their business, e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards. [24]

63. As a custodian of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

64. Defendants was, or should have been, fully aware of the unique type and the significant volume of data on Defendants server(s), amounting to millions of individuals detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

65. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

66. The ramifications of Defendants failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

67. As a company in possession of its Current/Former Employees' Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class

[24] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited June 10, 2025).

Members because of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employee-benefit management company or taxpayer identification number. [25]

69. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[26] For example, Personal Information can be sold at a price ranging from $40 to $200.[27] Criminals can also purchase access to entire company data breaches from $900 to $4,500. [28]

70. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans,

---

[25] *Id.*

[26] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited June 10, 2025).

[27] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 10, 2025).

[28] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 10, 2025).

credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud. [29]

71. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

72. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [30] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[31]

73. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone

[29] https://lifelock.norton.com/learn/identity-theft-resources/kinds-of-id-theft-using-social-security-number (last visited June 10, 2025).
[30] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases. (last visited June 10, 2025).
[31] *Id.*

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[32]

74. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[33] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[34]

75. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

76. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

77. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social

[32] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 10, 2025).
[33] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited June 10, 2025).
[34] *See* https://www.investopedia.com/terms/s/ssn.asp (last visited June 10, 2025).
[35] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 10, 2025).

Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target her in fraudulent schemes and identity theft attacks.")

78. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[36]

79. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name and Social Security number.

80. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

[36] *See* https://oag.ca.gov/idtheft/facts/your-ssn (last visited June 10, 2025).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[37]

81. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

82. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

83. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendants Fail to Comply with FTC Guidelines

84. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

---

[37] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 27, 2025).

[38] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited June 27, 2025).

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[39]

86. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[40]

87. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[39] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 10, 2025).
[40] *Id.*

89. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants duty in this regard.

90. Defendants failed to properly implement basic data security practices.

91. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

92. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of individuals; Defendants were also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Classes.

Defendants Owed Plaintiff and Class Members a Duty to Safeguard their Private Information

93. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with

industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

94. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in their possession, including adequately training their employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

95. Defendants owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

96. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

97. Defendants owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

98. Defendants owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft

99. The unencrypted Private Information of Plaintiff and Class Members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

100. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members.

101. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members because of the Data Breach.

102. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

103. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

104. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

105. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

106. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[41]

107. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[42]

108. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information

109. Private Information is valuable property.[43] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

110. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit

[41] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf. (last visited June 10, 2025).
[42] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.
[43] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited June 10, 2025) ("GAO Report").

or debit cards and obtaining replacements. The information stolen from the Data Breach is difficult, if not impossible, to change, such as dates of birth and Social Security numbers.

111. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[44]

112. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[45]

113. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[46] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[47,48] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[49]

114. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and

[44] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 10, 2025)

[45] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (last visited June 10, 2025)

[46] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited June 10, 2025)

[47] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited June 10, 2025).

[48] https://datacoup.com/ (last visited June 10, 2025)

[49] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last visited June 10, 2025)

diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

115. The fraudulent activity resulting from the Data Breach may not come to light for years.

116. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

117. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants network, amounting to millions of individuals detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

118. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

119. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank

accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

120. Such fraud may go undetected until debt collection calls commence months, or even years later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

121. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

122. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft resulting from Defendants Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear, but for Defendants failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

123. Furthermore, Defendants poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide Defendants with labor and their Private Information, Plaintiff and other reasonable employees understood and expected that they were, in part, exchanging their labor and Private Information for the necessary data security to protect the Private Information when, in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

Plaintiff Joshua Henderson's Experience

124. Plaintiff is a former employee of Defendants. As a condition of employment, he was required to provide his Private Information to Defendants.

125. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's Private Information in its system.

126. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

127. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking his bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

128. Following the Data Breach, Plaintiff noticed an uptick in spam calls, text messages, and emails.

129. As a result of the Data Breach, Plaintiff fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

130. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

131. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

132. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

133. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following Class and Subclass (collectively "the Classes"):

> **Nationwide Classes:** All individuals in the United States whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach, including all who were sent a notice of the Data Breach.

134. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family Members.

135. Plaintiff reserves the right to amend the definition of the Classes or add a Class or Subclass if further information and discovery indicate that the definition of the Classes should be narrowed, expanded, or otherwise modified.

136. **Numerosity.** The Class Members are so numerous that joinder of all Members is impracticable. Upon information and belief, more than 2.2 million individuals had their Private Information compromised in this Data Breach. The identities of Class Members are ascertainable through Defendants records, Class Members' records, publication notice, self-identification, and other means.

137. **Commonality.** Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual Class Members. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, are the following:

a. Whether and to what extent Defendants has a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants have respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants have respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

138. **Typicality.** Plaintiff's claims are typical of those of the other Class Members because Plaintiff, like every other Classes Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other Member of the Classes.

139. This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

140. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

141. **Superiority.** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually

afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

142. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

143. Adequate notice can be given to Class Members directly using information maintained in Defendants records.

144. Further, Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Whether Defendants owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendants security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendants failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendants failure to institute adequate protective security measures amounted to breach of an implied contract;

e. Whether Defendants failed to take commercially reasonable steps to safeguard Current/Former Employees' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

145. Plaintiff hereby repeats and realleges paragraphs 1 through 144 of this Complaint and incorporates them by reference herein.

146. Defendants require current and former employees, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of its business.

147. Defendants gathered and stored the Private Information of Plaintiff and Class Members in exchange for Defendants offer of employment.

148. Plaintiff and Class Members entrusted Defendants with their Private Information with the understanding that Defendant would safeguard their information.

149. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

150. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within them—to prevent disclosure of the information, and to safeguard the information from theft. Defendants duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

151. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

152. Defendants duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and Class Members entrusted Defendants with their confidential Private Information, a necessary part of being employed by Defendants.

153. Defendants duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect confidential Private Information.

154. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Classes.

155. Defendants breached their duties, thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, (a) failing to adopt, implement,

and maintain adequate security measures to safeguard Class Members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class Members' Private Information.

156. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly considering Defendants inadequate security practices.

157. It was foreseeable that Defendants failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

158. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

159. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants systems.

160. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

161. Plaintiff and Class Members had no ability to protect their Private Information that was in, and likely remains in, Defendants possession.

162. Defendants were in a position to protect against the harm suffered by Plaintiff and the Classes as a result of the Data Breach.

163. Defendants duty extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

164. Defendants have admitted that the Private Information of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach. Defendants waited nearly seven months after being made aware of the Data Breach, to notify individuals impacted.

165. But for Defendants wrongful and negligent breach of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

166. There is a close causal connection between Defendants failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendants failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

167. As a direct and proximate result of Defendants negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

168. As a direct and proximate result of Defendants negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

169. Additionally, as a direct and proximate result of Defendants negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

170. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

171. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(*On Behalf of Plaintiff and the Class*)

172. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 171 as though fully set forth herein.

173. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendants duty.

174. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

175. Defendants conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants systems.

176. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

177. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

178. As a result of Defendants negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

179. Plaintiff hereby repeats and realleges paragraphs 1 through 178 of this Complaint and incorporates them by reference herein.

180. Defendants offered to provide employment to its Current/Former Employees, including Plaintiff and Class Members, in exchange for labor.

181. Defendants also required Plaintiff and the Class Members to provide their Private Information to receive employment.

182. In turn, Defendants impliedly promised to protect Plaintiff's and Class Members' Private Information through adequate data security measures, including through the representations in their privacy policies.

183. Plaintiff and the Class Members accepted Defendants offer by providing Private Information to Defendants in exchange for employment.

184. Plaintiff and Class Members would not have entrusted their Private Information to Defendants but for the above-described agreement with Defendants.

185. Defendants materially breached their agreement(s) with Plaintiff and Class Members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

186. Plaintiff and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Defendants.

187. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in

connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. In other words, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

188. Defendants' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

189. The losses and damages Plaintiff and Class Members sustained as described herein were the direct and proximate result of Defendants' breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

COUNT IV
BREACH OF CONFIDENCE
(*On Behalf of Plaintiff and the Class*)

190. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 189 as though fully set forth herein.

191. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendants.

192. As alleged herein and above, Defendants relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

193. Plaintiff and the Class entrusted Defendants with their Private Information with the explicit and implicit understandings that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

194. Plaintiff and the Class also entrusted Defendants with their Private Information with the explicit and implicit understandings that Defendants would take precautions to protect that Private Information from unauthorized disclosure.

195. Defendants voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

196. As a result of Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

197. As a direct and proximate cause of Defendants actions and omissions, Plaintiff and the Class have suffered damages.

198. But for Defendants disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

199. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendants unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendants knew or should have known its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

200. As a direct and proximate result of Defendants breach of their confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket

expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

201. As a direct and proximate result of Defendants breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
(*On Behalf of Plaintiff and the Class*)

202. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 201 as though fully set forth herein.

203. Plaintiff and Class Members conferred a benefit upon Defendants by providing Defendants with their Private Information.

204. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendants also benefited from the receipt of Plaintiff's and Class Members' Private Information.

205. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because

Defendants failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendants had they known Defendants would not adequately protect their Private Information.

206. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grants the following:

A. For an order certifying the Classes, as defined herein, and appointing Plaintiff and his Counsel to represent the Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendants to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants network is compromised, hackers cannot gain access to other portions of Defendants systems;

x. requiring Defendants to conduct regular database scanning and security checks;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Defendants compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: June 27, 2025

Respectfully submitted,

By: */s/David M. Wilkerson*
David M. Wilkerson
WILKERSON JUSTUS PLLC
PO Box 54
Asheville, NC 28802
Tel: (828) 316-6902
Email: dwilkerson@wilkersonjustus.com

Mariya Weekes*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200
Fax: (786) 879-7520
Email: mweekes@milberg.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
Email : ostrow@kolawyers.com

Attorneys for Plaintiff and the Putative Classes

**Pro Hac Vice* forthcoming